

To Whom It May Concern:

I am writing in regards to the matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services. Enforcing this act in such a way that requires Internet service providers (ISP's) to assist law enforcement in easy surveillance of Voice over Internet Protocol (VoIP) communications is a very bad idea for three reasons.

First, it will be ineffective against anyone with a desire to hide their communication. As an IT professional, I know that the protocols are flexible enough to allow quick workarounds for any such surveillance attempts. Even if the ISP's are forced to provide keys to any encryption used at the network layer, the two parties communicating can encrypt the communication at the application level, rendering any surveillance worthless. Further, if the VoIP application happens to tunnel the traffic through another encrypted protocol, neither the ISP nor law enforcement will be able to distinguish such traffic from any other traffic. Consequently, my tax dollars will be wasted.

Second, this requirement will stifle innovation. Since the FCC will be mandating that ISP's do the technologically impossible, their resources will be spent complying rather than effectively implementing this new technology. Consequently, my broadband bill will be higher.

Third, since the public's protection against unjustified surveillance has been eroded with the PATRIOT act, such surveillance will undoubtedly be unfairly applied. Consequently, law-abiding citizens will be spied on while the terrorists and criminals slip right through the cracks.

Sincerely,
Ryan William Heffernan
Salt Lake City, Utah